(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 444 242 B1

(12) EUROPEAN PATENT SPECIFICATION

(45) Date of publication and mention of the grant of the patent:
07.02.2007 Bulletin 2007/06

(21) Application number: **02780463.2**

(22) Date of filing: **15.10.2002**

(51) Int Cl.:
G06Q 20/00 *(2006.01)*

(86) International application number:
PCT/US2002/032855

(87) International publication number:
WO 2003/042225 (22.05.2003 Gazette 2003/21)

(54) SECURE HANDLING OF STORED-VALUE DATA OBJECTS

SICHERE HANDHABUNG VON GESPEICHERTEN WERTDATEN OBJEKTEN

MANIPULATION SECURISEE D'OBJETS DE DONNEES A VALEUR STOCKEE

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LI LU MC NL PT SE SK TR

(30) Priority: **13.11.2001 US 8174**

(43) Date of publication of application:
11.08.2004 Bulletin 2004/33

(60) Divisional application:
05110957.7 / 1 632 917

(73) Proprietor: **Ericsson Inc.**
Plano, Texas 75024 (US)

(72) Inventors:
- **DUTTA, Santanu**
  Cary, NC 27513 (US)
- **RYDECK, Nils**
  Cary, NC 27511 (US)

(74) Representative: **Lundqvist, Alida Maria Therése et al**
Dr. Ludwig Brann Patentbyra AB,
P.O. Box 171 92
104 62 Stockholm (SE)

(56) References cited:
EP-A- 0 980 052 **EP-A- 1 132 839**
WO-A-00/74300

- **KURAMITSU K ET AL: "TTP: secure ACID transfer protocol for electronic ticket between personal tamper-proof devices" COMPUTER SOFTWARE AND APPLICATIONS CONFERENCE, 2000. COMPSAC 2000. THE 24TH ANNUAL INTERNATIONAL TAIPEI, TAIWAN 25-27 OCT. 2000, LOS ALAMITOS, CA, USA,IEEE COMPUT. SOC, US, 25 October 2000 (2000-10-25), pages 87-92, XP010523749 ISBN: 0-7695-0792-1**
- **MATSUYAMA K ET AL: "DISTRIBUTED DIGITAL-TICKET MANAGEMENT FOR RIGHTS TRADING SYSTEM" PROCEEDINGS ACM CONFERENCE ON ELECTRONIC COMMERCE, XX, XX, 1999, pages 110-118, XP001130642**
- **FUJIMURA K ET AL: "Digital-ticket-controlled digital ticket circulation" PROCEEDINGS OF THE EIGHTH USENIX SECURITY SYMPOSIUM (SECURITY'99), PROCEEDINGS OF 8TH SECURITY SYMPOSIUM, WASHINGTON, DC, USA, 23-26 AUG. 1999, pages 229-238, XP002251321 1999, Berkeley, CA, USA, USENIX Assoc, USA**

Note: Within nine months from the publication of the mention of the grant of the European patent, any person may give notice to the European Patent Office of opposition to the European patent granted. Notice of opposition shall be filed in a written reasoned statement. It shall not be deemed to have been filed until the opposition fee has been paid. (Art. 99(1) European Patent Convention).

EP 1 444 242 B1

Description

BACKGROUND OF THE INVENTION

[0001] The present invention generally relates to conducting secure transactions, and particularly relates to securely managing wireless device transactions involving stored-value data objects.

[0002] As portable electronic devices become more fully integrated into the everyday lives of people, these devices will be used in a broader range of transactions. For example, one might integrate payment functions into a portable communication device such as a cellular telephone. A user can then pay for selected goods or services using the phone's payment functions.

[0003] Security issues complicate using portable devices in commercial transactions. For example, if the user's device contains payment information, how is that information conveyed to a vendor system in a manner secure from unwanted eavesdropping or monitoring? In general, significant issues arise in providing end-to-end security for such transactions.

[0004] Particular challenges arise in securely delivering and retrieving information to and from a portable device. The need for such delivery and subsequent retrieval might arise in the context of delivering a stored-value data object to the device for later redemption by the user. Here, the data object might function analogous to a physical ticket. Indeed, a vendor might issue an electronic ticket or other token for delivery to the user's device for subsequent redemption. Upon redemption of the electronic ticket, the user gains access to or receives the desired goods or service.

[0005] EP-A-1132839 describes a prior art system to securely manage stored-value data objects comprising an issuing system, a security element in a user device and a redeeming system.

[0006] However, the use of electronic tickets or other stored-value data objects requires significant security provisions throughout the issuing and redeeming processes. An approach to securely managing the use of stored-value data objects with portable devices requires a solution that addresses these and other security concerns. Yet, any such approach should make the use of such data objects relatively convenient and flexible from the user's perspective.

BRIEF SUMMARY OF THE INVENTION

[0007] The present invention provides methods and apparatus for securely managing wireless device transactions involving the use of stored-value data objects. In some embodiments, the stored-value data object functions as an electronic ticket or token, and methods and apparatus are provided for securely issuing, storing, and redeeming the electronic ticket.

[0008] In at least one embodiment, the wireless device requests a desired stored-value data object from a ticket issuing system. The ticket issuing system ensures secure delivery to the requesting device by encrypting the requested data object using a public key provided by the wireless device in association with the request. Only the requesting wireless device has the corresponding private key, and thus only that device can decrypt and subsequently use the data object. The wireless device may include a security element, which offers tamper-resistant, secure decrypting and storage for the data object, and secure storage of the private key.

[0009] The ticket issuing system may offer local access, in which case the wireless device might use RF or optical (e.g., infrared) signaling to communicate with the ticket issuing system. In at least one embodiment, the ticket issuing system is a remote server or other system accessible through the Internet, and the wireless device accesses it through a wireless communication network. For example, the device might incorporate a RF transceiver adapted to communicate with a cellular communication network. Communication between the internet-based ticket issuing system and the wireless device might use the Wireless Application Protocol (WAP). If WAP is used, the wireless device might provide its associated public key to the ticket issuing system in a user certificate, in accordance with WAP Public Key Infrastructure (WPKI) methods.

[0010] After receiving the stored-value data object (e.g., electronic ticket) in encrypted form from the ticket issuing system, the wireless device transfers the encrypted data object to its security element, which may be integrated in the wireless device or removeably connected therewith. In any case, the security element provides for secure storage of the data object and does not permit viewing, retrieving, or otherwise modifying the stored data object except in accordance with its security rules. As noted, the security element also may provide secure storage of the private key used to decrypt the data object as received from the ticket issuing system. Additionally, the security element may allow a user of the wireless device to browse or view selected fields or portions of the stored data object, but prevents unauthorized copying of the stored data object by not allowing unencrypted access to the full data object.

[0011] Once the security element contains a stored data object, such as an electronic ticket, the wireless device user can redeem the data object for associated goods or services at a compatible ticket redeeming system. The ticket redeeming system ensures that the data object being redeemed is valid, and cooperates with the security element in the redeeming wireless device to ensure that unauthorized copies of the stored data object cannot be extracted by eavesdropping on the communication between the wireless device and the ticket redeeming system. Further, the security element in the wireless device ensures that unauthorized copies of the stored-value data object are deleted or otherwise not retained. Communication between the wireless device and the ticket redeeming system may use RF, infrared, or other wireless

signaling. In at least one embodiment, the wireless device includes an RF interface, such as a Bluetooth interface, for communicating with the ticket redeeming system. Communication between the ticket redeeming system and the wireless device may be based on WAP, or on other standardized or proprietary protocols.

[0012] In at least some embodiments, the wireless device initiates redemption of the stored data object by sending a redemption request to the ticket redeeming system. The wireless device may also provide its associated public key to the ticket redeeming system as part of this request. In response, the ticket redeeming system sends a certificate containing its associated public key to the wireless device. The ticket redeeming system may also send a nonce ("number used once") or other generated value (e.g. pseudorandom value) to the wireless device.

[0013] The security element encrypts a combination of the generated value supplied by the redeeming system and the ticket using the public key received from the redeeming system. The wireless device then sends the encrypted data object to the ticket redeeming system using whatever protocols are associated with the particular interface used to communicate with the ticket redeeming system. Generally, these protocols should support transmission verification to insure that the ticket redeeming system successfully receives the encrypted data object. Upon transmitting the data object to the ticket redeeming system, the security element in the wireless device erases or otherwise clears its stored copy of the data object.

[0014] The ticket redeeming system decrypts the received data object using a private key corresponding to the public key it provided to the wireless device. During decryption, the ticket redeeming system separates the data object from the nonce and verifies that the data object contains an authentic signature or other marking data from a legitimate ticket issuing system, or from a legitimate ticket redeeming system. If the data object is a multi-use object, such as a multi-use electronic ticket, the ticket redeeming system alters the data object as required, signs it with its own private key, and then returns it in encrypted form to the wireless device, where it is decrypted and stored in the security element, ready for subsequent redemption.

[0015] In any case, the ticket redeeming system may offer or otherwise enable access to the goods or service associated with redeeming the data object, such as by opening a gate or by returning a rapid verification token (RVT), in exchange of the data object, to the wireless device for subsequent use in accessing the goods or service. A RVT as defined herein typically comprises a different type of information than the data object discussed above, and has associated transfer and verification procedures making it amenable to quick verification.

[0016] A RVT might be used in situations where one or more subsequent rapid verifications are desired after initial redemption of a stored data object using full security. For example, a ticketed passenger might use his or her portable device to perform full redemption of a stored electronic ticket at a ticket redeeming system positioned in advance of the boarding area. Upon redeeming the electronic ticket, the ticket redeeming system returns a RVT to the passenger's portable device, which may then be rapidly verified immediately prior to boarding the aircraft. Of course, usage of RVTs extends to a broad range of other activities such as enforcing ticketed access at sporting events.

[0017] In at least some embodiments, the ticket redeeming system returns a seed value to the wireless device, and may optionally return graphical data or pattern generating information. The seed value may be a pseudorandom value. The security element in the wireless device uses the returned seed value to drive some form of pattern or sequence generator. The pattern/sequence generator preferably incorporates time-of-day dependency in its generation function, such that the sequence or pattern generated by it depends on both the seed value and the time-of-day. If a human operator is meant to redeem or authenticate the RVT, the security element can generate an authentication pattern or otherwise manipulate a graphical element that it displays in a manner dependent upon the seed value, and on time-of-day if desired. Thus, only security elements having valid seed values are able to present the proper pattern or graphical manipulation to the verifying human operator at the verification instant.

[0018] Incorporating time-of-day considerations into sequence/pattern generation functions protects RVT verification against replay attacks. In general, the pattern/sequence generator generates the desired pattern or sequence at the time of verification. In so doing, the time-of-day used in generation is very close to current time. For example, the pattern/sequence might be generated a half-second before actual verification. Verification might then be made to depend on the time-of-generation being within a certain window of time. This dependency prevents a user from outputting an otherwise valid verification pattern or sequence for recording and subsequent playback to a verifying system.

[0019] Where a subsequent automated system is meant to verify the RVT, the wireless device may simply transmit a verification sequence to the verifying system. Generally, the verification sequence contains at least one pseudorandom element generated in dependence on the seed value, and preferably also in dependence on the time-of-day. The verifying system receives the verification sequence and checks its validity. It does so by locally generating the same pseudorandom element or elements in the verification sequence, which is feasible because the verification system has knowledge of the seed value that was transmitted to the wireless device by the ticket redeeming system. This seed value is used system-wide, that is, it is given to all wireless devices over a moderately long pre-determined period of time. The period of time may be much longer than the typical user delay between redeeming the ticket at the first TRS and

subsequently redeeming the RVT. The RVT-checking TRS would allow acceptance of both the present and the previous period seeds over a relatively brief period following a seed-change; this would accommodate users who obtained their seed just prior to a seed change.

[0020] If the pseudorandom element is generated in dependence of time-of-day as well as the seed value, the wireless device may transmit the time-of-day it used in generating the pseudorandom element included in its verification sequence. The verifying system can use this received-time-of-day value and the known seed value to generate its own pseudorandom element for comparison against the pseudorandom element received from the wireless device. Further, the verifying system may qualify the time-of-day received from the wireless device to make sure it is not old (i.e., stale).

[0021] Alternatively, verifying system may be synchronized to the same time reference as the wireless device, such that the time-of-day maintained by the verifying system closely matches the time-of-day maintained by the wireless device. If such synchronization is not desirable, the verifying system may allow for a defined time variance between it and the wireless device. In any case, the verifying system may also use the time-of-day in determining whether a received verification sequence is valid, thus preventing a given verification sequence from being copied and reused by other wireless devices.

BRIEF DESCRIPTION OF THE DRAWINGS

[0022]

Fig. 1 is a diagram of an exemplary system supporting the secure handling of stored-value data objects in accordance with the present invention.

Fig. 2 is a more detailed diagram of an exemplary embodiment of the system of Fig. 1.

Fig. 3 is a diagram of exemplary embodiments of the ticket issuing system, ticket redeeming system, and personal trusted device shown in Figs. 1 and 2.

Fig. 4 is an exemplary call flow diagram detailing the issuance and redemption of electronic tickets or other types of stored-value data objects.

Fig. 5 is a diagram of an exemplary environment suited for the use of rapid verification tokens.

Fig. 6 is a diagram of an exemplary verification display associated with a rapid verification token.

DETAILED DESCRIPTION OF THE INVENTION

[0023] The present invention provides systems and methods enabling certain transactions related to wireless e-commerce. The following detailed description and accompanying drawings provides specific, exemplary details regarding implementations for at least some embodiments of the present invention. However, the scope of the present invention extends well beyond these specific details. For example, it should be understood that where wireless communication systems are involved, no particular wireless communication interface standard is necessary for practicing the present invention.

[0024] Moreover, the discussion below refers specifically to electronic tickets, but this term should be understood to be a particular embodiment of the more general concept of any stored-value data object. Thus, the term "electronic ticket" as used herein encompasses other stored-value data objects, such as electronic cash, electronic tokens, and any other data item or object that may be used as a medium of exchange in e-commerce, and in other for-value transactional activities.

[0025] Figure 1 illustrates a simplified, exemplary system 10 for practicing one or more embodiments of the present invention. System 10 comprises a ticket issuing system (TIS) 12, a ticket redeeming system (TRS) 14, and a user device 16. In this context, the user device 16 is referred to herein as a "personal trusted device" (PTD) 16. The PTD 16 contains a security element 20, which is adapted to act as a trusted agent of the TIS 12 and TRS 14 in stored-value data object transactions, such that the security element 20 cooperates with the TIS 12 and TRS 14 in securely issuing, storing, and redeeming an electronic ticket 18. It should be understood that the PTD 16 represents essentially any device type having the appropriate wireless communication capabilities. Thus, PTD 16 might be an appropriately configured radiotelephone or other mobile terminal, personal digital assistant, hand-held, laptop, other personal computer device, or other type of electronic device.

[0026] In managing the secure transfer, handling, and redemption of electronic tickets, the systems and processes used must ensure reliable and convenient electronic ticket generation, issuance, and redemption, which includes preventing fraud and misuse. In general, the TIS 12, TRS 14, and security element 20 cooperate to achieve the following goals:

- The ticket recipient must be assured that the ticket issuer is legitimate.
- The ticket must be delivered only to the legitimate user, i.e., it shall not be possible for a person other than the user to receive and make use of the ticket.
- The ticket must be prevented from copying by the user, whether such copying might be undertaken legitimately or fraudulently.
- The user must be assured that the ticket collector (redeeming system) is legitimate.
- The ticket must be delivered only to the legitimate ticket collector, i.e., it shall not be possible for an entity other than the legitimate ticket collector to receive and make use of the ticket.
- The ticket collector must have a reliable mechanism for ensuring that the ticket is legitimate.
- If the ticket collector returns the ticket to the user, it must ensure that the ticket is delivered only to the legitimate user, i.e., it shall not be possible for a person other than the user to receive and make use of

the returned ticket.

[0027] In addition to the above secure handling requirements, rapid ticket verification is also a requirement in many ticketing services. Rapid verification is especially advantageous in mass transit systems, sports events, concerts, etc. With rapid verification, which is discussed in more detail later, there may be a tradeoff between verification security and verification speed. In general, the concept entails subjecting an electronic ticket to a high level of initial security to insure verification, and then providing the user with a potentially less secure, short-lived, rapid verification object that may be subsequently verified more quickly than the original electronic ticket.

[0028] Figure 2 is a more detailed illustration of an exemplary embodiment of secure ticket transactions. In this instance, the PTD 16 may be a mobile terminal or other cellular radiotelephone. As such, the PTD 16 wirelessly communicates with the TIS 12 by accessing the wireless communication network 22, which typically comprises an access network (AN) 26 and a core network (CN) 28. The wireless communication network 22 provides access to the TIS 12 via the internet 24 or by some other network connection. The wireless communication network 22 may be any one of a number of standardized network implementations, including GSM, CDMA (IS-95, IS-2000), TDMA (TIA/EIA-136), wide band CDMA (W-CDMA), GPRS, or other type of wireless communication network.

[0029] Any number of end-to-end protocols may be used in supporting ticketing transactions conducted between the PTD 16 and the TIS 12. For example, the TIS 12 may be a WAP-enabled server, thereby allowing WAP-enabled PTDs 16 to conduct ticketing transactions with the TIS 12 based on WAP standards in conjunction with special MIME types defined for the ticketing messages. In particular, the reader is referred to the standards document entitled "Wireless Application Protocol Public Key Infrastructure Definition," WAP-271-WPKI, Version 24-Apr-2001, as promulgated by the WAP Forum. Of course, other protocols may be used, and indeed numerous open and proprietary protocols are available for supporting transactions between the PTD 16 and the TIS 12.

[0030] Moreover, it should be understood that while configuring the TIS 12 as an Internet-accessible ticket issuing system is attractive in terms of flexibility and broad access, the TIS 12 might be implemented as part of the wireless communication network 22. For example, the TIS 12 may be implemented as one of a number of network entities within the core network 28. In that case, some security concerns associated with the TIS 12 are eliminated, or at least minimized, but access to the TIS 12 may be more restricted. For example, the TIS 12 might be accessible only to subscribers of the wireless communication network 22.

[0031] Once the PTD 16 receives an electronic ticket from the TIS 12, it transfers the ticket 18 to its security element 20, where it is decrypted and securely held for subsequent redemption. To that end, the PTD 16 further supports wireless communication with the TRS 14 for redemption transactions. The TRS 14 may be linked to other systems via a supporting network 30, and in fact may be connected to one or more of the Internet 24, the TIS 12, and the wireless communication network 22. While not shown, it should be understood that the TRS14 may also be linked directly or indirectly to other TRSs 14, and to other types of equipment associated with ticket redemption, and, optionally, may be linked with rapid verification systems discussed later herein.

[0032] Figure 3 provides more detail regarding exemplary embodiments of the TIS 12, the TRS 14, and the PTD 16. Additionally, Fig. 3 defines exemplary information exchanged between the PTD 16 and the TIS 12 and TRS 14.

[0033] Specific embodiments of the PTD 16 will vary significantly because the term "PTD", as used herein, encompasses a broad range of device types. In an exemplary embodiment, the PTD 16 comprises a functional element 40 and wireless interfaces 40 and 42, in addition to the security element. As used herein, the term "functional element" essentially describes the whole of the PTD 16 apart from the security element 20. As will be explained later, the PTD 16 may use the same wireless interface 42 or 44 to communicate with both the TIS 12 and the TRS 14, but will oftentimes incorporate separate wireless interfaces. Generally, the need for different wireless interfaces is determined based on whether the TIS 12 and the TRS 14 are both local systems, both remote systems, or a mix of remote and local systems. For example, as described earlier, the PTD 16 may communicate with the TIS 12 using WAP services supported by the wireless communication network 22, while communicating with the TRS 14 at a redemption site via a local communication link.

[0034] The characteristics of functional element 40 will vary depending upon the nature of the PTD 16. That is, functional element 40 may be a cellular telephone, a personal digital assistant (PDA), or other type of electronic device dependent on the intended purpose of the PTD 16 in question. Generally, the functional element 40 comprises some type of processor or processors 50, memory 52, a user interface 54 and a real-time clock (RTC) 56. Details of the user interface 54 also vary with the intended purpose of the PTD 16. For example, if the PTD 16 is a cellular telephone or other mobile terminal, the user interface 54 typically comprise a display screen, keypad, and audio input/out systems. Similarly, if the PTD 16 is a PDA or other mobile computing device, the user interface 54 generally includes display and input/output functions.

[0035] The security element 20 in the PTD 16 may be implemented in any number of ways. For example, the security element 20 may be integrated with the other systems of the PTD 16, or may be a removable smart card or other modular device. In any case, the security element

20 may be implemented as a tamper-resistant secure module that provides for highly secure storage of electronic tickets and other sensitive data. In an exemplary embodiment, the security element 20 comprises a processor, or other logic 60, memory 62, and a sequence/pattern generator 64. Functions associated with the security element 20 are described in more detail later in association with describing transactions involving the TIS 12 and TRS 14.

[0036] In an exemplary embodiment, the TIS 12 comprises a WAP-enabled server, or other network-accessible ticket issuing system. In general, the TIS 12 includes an interface 70 configured for the type of network with which the TIS 12 communicates. In some embodiments, the interface 70 may include wireless communication functionality to support local wireless communication with PTDs 16. The TIS 12 further comprises a processing/encryption system 72 and memory 74.

[0037] Similarly, the TRS 14 comprises an interface 80, a processing system 82 providing encryption and decryption services, and memory 84. Of course, both the TIS 12 and the TRS 14 may be implemented differently depending on the specific capabilities and communication methods desired.

[0038] Independent of the above implementation details, a typical electronic ticket transaction involves a purchase request from the PTD 16 to the TIS 12, and subsequent delivery of the requested electronic ticket 18 from the TIS 12 to the PTD 16. Later, a user of the PTD 16 presents the electronic ticket 18 to the TRS 14 for redemption. A number of mechanisms are used within the present invention to ensure end-to-end security for issuing, storing, and redeeming electronic tickets (i.e., stored-value data objects).

[0039] Figure 4 illustrates an exemplary call flow that might be practiced in one or more embodiments of the present invention. The overall set of electronic ticket transactions begins with the PTD 16 generating and transmitting a purchase request for receipt by the TIS 12. A user certificate that includes a public key associated with the PTD 16 is transmitted in conjunction with the purchase request, or is otherwise made available to the TIS 12. The PTD certificate may be a certificate issued by the operator of the TIS 12 or an associated system, or may come from a trusted third party such as VISA or MASTERCARD. In any case, once the TIS 12 is assured of payment for the electronic ticket 18, which procedures are not germane to the present invention, it generates the requested electronic ticket 18.

[0040] Referring back to Fig. 3 it might be noted that the ticket 18 may be generated and held in memory 74. Once the ticket 18 is generated with the desired content and signed or otherwise authenticated by the TIS 12, it is encrypted using the public key (PTD_{PuK}) associated with the requesting PTD 16. Because only the requesting PTD 16 has the corresponding private key, only the requesting PTD 16 will be able to receive and make use of the encrypted ticket 18. Thus, at Step A in Fig. 4, the TIS 12 issues the requested electronic ticket 18 in encrypted format. Note that the ticket 18 consists of data that is digitally signed by the TIS 12, the digital signature being performed by encrypting the ticket data (TICKET_DATA) with a private key (TIS_{PrK}) belonging to and securely held by the TIS 12.

[0041] The PTD 16 receives the encrypted ticket 18 via the wireless interface 42, and may pass the encrypted ticket 18 directly to the security element 20, or indirectly through the functional element 40. In one embodiment, the TIS 12 sends the encrypted electronic ticket to the PTD 16 as a special Multipurpose Internet Mail Extension (MIME) type, which message type triggers the transfer of the encrypted ticket 18 to the security element 20. In any case, the security element 20 decrypts the received ticket 18 using its securely held private key. The security element 20 may hold a root certificate (TIS_ROOT_CERT) corresponding to the TIS 12, which certificate includes the private key needed to decrypt the electronic ticket 18 received from the TIS 12.

[0042] The decrypted ticket 18 is held in security element memory 62. It is noteworthy that the security element's fixed, pre-defined input/output functions never yield the decrypted electronic ticket 18 to the outside world. Hence, the ticket 18 stored in the security element 20 is inaccessible to would-be copiers, although the security element 20 may make selected fields or portions of the ticket 18 available for browsing by the user of PTD 16.

[0043] Subsequent to receiving the ticket 18 from the TIS 12, the user of the PTD 16 presents the electronic ticket 18 to the TRS 14 for redemption. Ticket redemption typically begins with the PTD 16 issuing a redemption request to the TRS 14, which might take the form of a WAP Session Protocol (WSP) Get request from the PTD 16 to the TIS 12, as shown in Fig. 4 by the Get_Service message. The above Get message may be issued as a result of the user independently navigating to a TIS website, or by the receipt by the PTD 16 of a WAP Push message issued by the TIS 12, containing the url of the TIS 12, and the user selecting the said url on his PTD.

[0044] As was mentioned early, the PTD 16 preferably communicates with the TRS 14 wirelessly through wireless interface 42 or 44. If the TRS 14 is remote, the PTD may access it as it would a remote TIS 12 through the wireless communication network 22, in which case the PTD 16 uses wireless interface 42. If the TRS 14 is local, the PTD 16 uses wireless interface 44, which may comprise a radio frequency interface, an optical interface, some combination thereof, or may be based on some other wireless technology. Wireless technologies of particular interest in this context include Bluetooth and 802.11 wireless networking standards, and additionally include the infrared communications standards promulgated by the Infrared Data Association (IrDA). Of course, it should be understood that communication between the PTD 16 and the TRS 14 might be based on other standards, including proprietary communication protocols.

[0045] Upon receiving the redemption request from the PTD 16, the TRS 14 sends a message, B, termed "Request To Show Ticket" to the PTD 16, which request includes a generated value and a certificate ($Cert\_TRS^{n+1}$) associated with the particular TRS 14. The generated value may be a nonce, for example. The certificate transferred from the TRS 14 to the PTD 16 includes a public encryption key (TRS_{PuK}) associated with the TRS 14.

[0046] In response, the security element 20 within the PTD 16 creates a composite data object, (Nonce, T), comprising the received generated value concatenated with the electronic ticket 18. This composite data object is then digitally signed by the PTD 16 using the private key of the PTD 16. Preferably, a standard format such as PKCS 7, is used, whereby the certificate containing the PTD's public key, Cert_PTD, is appended to the signed object. The signed composite data object is then encrypted with the public key belonging to the particular TRS 14, the said public key being contained in the certificate, $Cert\_TRS^{n+1}$, sent from the TRS 14 to the PTD 16 in message B in the previous step. In this discussion, the present TRS 14 is identified by index number (n+1) and a previous TRS, for multi-use tickets, by (n).

[0047] Following encryption of the signed composite data object, the PTD 16 returns the encrypted composite object to the TRS 14. For multi-use tickets described below, the certificate of the previous ticket redeeming system, $Cert\_TRS^{n}$, is also sent as a component of message C. The TRS 14 decrypts the received generated value and electronic ticket 18 using the corresponding private key (TRS_{PrK}), known only to that TRS 14, and checks the authenticity and integrity of the received electronic ticket, as well as verifies the returned generated value.

[0048] In particular, the TRS 14 checks whether the received electronic ticket includes an authentic signature or other verification information from a legitimate TIS 12 and/or from another TRS 14, which might have signed a multi-use ticket after modifying it, as described below. In so checking, the TRS 14 may use a locally stored copy of the root certificates of one or more TISs 12 and the certificate of the previous TRS received from the PTD 16.

[0049] The TRS 14 may also check the PTD's signature on the composite data object returned by the PTD 16 to verify possession by the PTD 16 of the private key corresponding to the public key contained in the submitted PTD certificate.

[0050] If the electronic ticket 18 being redeemed at the TRS 14 is a one-time use ticket, the TRS 14 verifies that the ticket is valid and provides a signal or other indication to an associated system that the presenter of the ticket 18 should be granted access to the goods or service corresponding to the received ticket 18, or that a RVT should be issued. In conjunction with transmitting the ticket 18 from the PTD 16 to the TRS 14 in association with its redemption, the security element 20 erases the secure copy of the ticket 18 that it holds within its memory 62. This prevents unauthorized duplicate copies of the ticket 18 remaining during or after redemption.

[0051] In some instances, the electronic ticket 18 is a multiple use ticket. If so, the TRS 14 may return a redeemed ticket 18'. The redeemed ticket 18' may comprise a "punched", that is, an altered copy of the original electronic ticket 18. For example, the TRS 14 may modify the original electronic ticket 18 to show that it has been redeemed for the *n*th time, where *n* is a number from one (1) to the maximum number of times that the ticket 18 may be used. In returning a multi-use ticket 18', the TRS 14 may modify the ticket contents to contain an authentication signature associated with the TRS 14, which may be used to verify the redeemed ticket 18' at subsequent verification points.

[0052] In some cases, the result of redeeming a ticket 18 will be the issuance of a rapid verification object by the TRS 14. The PTD 16 receives the rapid verification object, and later uses it to generate a RVT, which may be quickly validated, albeit with less security, at a subsequent verification point. The rapid verification object sent from the TRS 14 to the PTD 16 itself might comprise the RVT, which is presented by the PTD 16 at a later verification point, but typically, the rapid verification object is a seed value, possibly with other information, from which the PTD 16 generates a valid RVT. Other information sent by the TRS 14 as part of the rapid verification object may include image data, image manipulation information, user-identifying data, etc. In any case, the TRS 14 might, depending on circumstances, return a redeemed ticket 18', a rapid verification object, neither, or both.

[0053] The use of RVTs might arise in association with tickets 18 issued for sporting events or for use at train stations, for example. In this instance, an original electronic ticket 18 might be subject to verification at a TRS 14 positioned at an open access area, whereupon the TRS 14 returns a rapid verification object to the redeeming PTD 16, which object, used in generating the RVT, may remain valid only for a defined period of time or a defined number of subsequent RVT validations.

[0054] Figure 5 illustrates more specifically an environment where RVTs might be useful. One or more TRSs 14 are available in an open area where users of PTDs 16 may initially redeem their electronic tickets 18. This initial redemption is typically a high security process, for example, one performed in accordance with the above description. The TRSs 14 return rapid verification objects to PTDs 16 redeeming valid electronic tickets 18. The PTD users may then present RVTs from their PTDs 16 to gain access to a controlled access area, for example. Arrangements of this sort are particularly useful in circumstances where event attendees or service users arrive at staggered times in advance of the event or service, and then subsequently queue up at a particular time. One might imagine the usefulness of the combination of high security verification followed by a subsequent lower security but faster verification at airport terminals, and at other mass transit facilities.

[0055] RVTs may be verified by rapid verification sys-

tems 100, but might also be verified by human operators. It should be understood that rapid verification systems 100 might simply be implemented as TRSs 14 but adopting both the secure verification protocols discussed earlier as well as lower-overhead rapid verification protocols. When returning rapid verification information to PTDs 16 from TRSs 14, the TRSs 14 may include a variety of data elements. In exemplary embodiments, the TRS 14 returns at least a seed value, and may also return visual pattern generating information, image information, and one or more associated scripts, the use of which information is explained below.

[0056] In one approach, the TRS 14 returns an image and a seed value in encrypted format as the rapid verification object to the PTD 16. The security element 20 in the PTD 16 includes a sequence/pattern generator 64 capable of generating pseudorandom sequences, or visual pattern information for display on the PTD screen, using the returned seed value. Additionally, the sequence/pattern generator 64 may be adapted to generate pseudorandom sequences based not only on this returned seed value, but on the time of day value that might be obtained from the real-time clock 56, for example. In many instances, the RTC 56 is itself synchronized to an overall network time or other referenced time, such as a GPS-based reference time. By making the RVT presented by the PTD 16 for verification dependent on time-of-day, the ability to fraudulently replay an earlier-generated RVT is eliminated.

[0057] In an exemplary scenario, a time-varying image is generated by the security element 20 in the PTD 16 by one of two approaches. A bit-mapped core image, which may be in data-compressed form, is transmitted from the TRS 14 to the PTD 16; this image is then manipulated by a program (e.g., computer instructions) native to the security element 20. This security element program takes as its inputs the output from the sequence/pattern generator 64, and the time time-of-day output or derived from the RTC 56. Alternatively, the program for creating and manipulating the time-varying image is itself sent from the TRS 14 to the PTD 16, possibly in compressed data form. This latter alternative is more suitable when the displayed image is an abstract, computer-generated pattern. It is noteworthy that the verification image displayed by the PTD 16, regardless of how it is generated, should have the qualities of easy human recognition, including clear discrimination among its various manipulated forms.

[0058] Figure 6 illustrates one embodiment of a human-verifiable RVT. The depicted images may be displayed on a display screen included within the user interface 54 in the PTD 16. In this exemplary embodiment, the displayed image includes (a) the user's picture, which is typically static; (b) a recognizable pattern that changes at discrete time intervals; and (c) a recognizable pattern changing continuously with time.

[0059] The user's picture in (a) above is accessed by the TRS 14 from a server whose location address, as typified by an Internet url, is contained in the PTD certificate sent by the PTD 16 to the TRS 14 in message C in association with signing the composite data object. This image, possibly in compressed form, is forwarded by the TRS 14 to the PTD 16 as a part of the rapid verification object (RVO) in message D.

[0060] As an example of (b) and (c), the illustration of Fig. 6 shows a wine glass and ball in association with the user's image. The wine glass takes on a series of rotational angles, wherein the sequence of rotational angles assumed by the wine glass are determined by the sequence/pattern generator 64, based on the seed value provided by the TRS 14 and a time-of-day value. The wine glass image changes at discrete time instants which are sufficiently spaced to allow easy human verification. The exemplary time interval shown in Fig. 6 is 30 seconds. In this case, the defense against replay attack is the presence of the user's picture as a component of the verification image displayed by the PTD 16.

[0061] Regarding the image component (c), it may be advantageous to pick the ball as following a circular orbit in an essentially continuous motion where the direction of rotation of the ball is determined by a pseudorandom sequence, and the position of the ball in its circular path is determined by the time-of-day. A continuously varying component in the verification image provides a defense against replay attacks comprising real time monitoring and rebroadcast of the image to multiple fraudulent users.

[0062] The human operator may have a rapid verification system 100, such as a hand-held device, having a display with similar images following the same pseudorandom sequence or sequences. In this manner, the human operator can look at the PTD's display and compare the verification image depicted there with the reference image displayed by the rapid verification system 100.

[0063] In ensuring that the displayed patterns on the rapid verification system 100 remain in sync with the patterns being generated by PTD 16 having valid RVTs, the rapid verification system 100 may synchronize its time of day to the same time reference used by the security element 20 in the PTD 16. Thus, the rapid verification system 100 may synchronize its time of day to a network time of day, such as the time maintained by the wireless communication network 22, or may also have a GPS-based time reference. Alternatively, the rapid verification system 100 may simply maintain a very accurate time of day, and allow for slight variations between its time of day and the times of day in the PTD 16. Thus, slight discrepancies between the PTD image and the verification image may be tolerated.

[0064] As mentioned earlier, an alternative approach has the PTD 16 provide the time-of-day to the rapid verification system 100. This allows the rapid verification system 100 to use the same time-of-day value as was used by the security element 20 in generating pseudorandom data from the seed value. With this approach, the rapid verification system can determine whether the time-

of-day value provided by the PTD 16 is recent enough to be deemed legitimate. That is, if the time-of-day value received from the PTD 16 is too old, the rapid verification system 100 can reject the verification sequence or pattern provided to it as being a replay of an earlier verification sequence.

[0065] Use of a verification sequence is particularly well suited where verification is performed using automated processing. Thus, the RVT generated by the security element 20 and transmitted from the PTD 16 to the rapid verification system 100 might simply be a verification sequence having at least one pseudorandom element generated in dependence on the seed value provided by a legitimate TRS 14 and a PTD time-of-day. The verification sequence can include additional, non-pseudorandom information, such as protocol-defined headers, etc. As with the human-readable version, the rapid verification system 100 may determine whether a sequence is valid based on the known seed value and a synchronized time of day.

[0066] If the rapid verification system's time of day is not synchronized to the same reference used by the security element 20, rapid verification system 100 may compare the received sequence to one of several valid sequences representing a defined time window. In this matter, absolute synchronization of times between PTD 16 and rapid verification system 100 is not necessary; however, by defining the non-discrepancy tolerance to be suitably small (e.g., ± 2 seconds), the rapid verification system 100 ensures that an earlier issued seed value has not been redistributed to another PTD 16 for fraudulent reuse.

[0067] As noted in detail above, the PTD 16 may include the actual time-of-day value used by the security element 20 in generating the pseudorandom element or elements as a preamble in the verification sequence it transmits to the rapid verification system 100. This technique is useful in that the rapid verification system's time-of-day may not exactly match the time-of-day reference used by the security element 20. The rapid verification system 100 will check the received verification sequence against its own reference sequence for the PTD-declared time-of-day (i.e., for the time-of-day value received from the PTD). If the received verification sequence is valid, this proves that the PTD 16 (security element 20) had the correct seed value. The rapid verification system 100 will then decide if the PTD-declared time-of-day is within acceptable limits of clock inaccuracy and processing delay. Verification sequences reflecting excessive delays would be rejected as they might result from replay fraud.

[0068] In an alternate exemplary approach, the rapid verification object returned by the TRS 14 is a paper ticket or other physical token that may be redeemed by the PTD user. In this approach, the TRS 14 may mark the physical token with authentication indicia that may change with time to prevent token reuse.

[0069] Given the broad scope of the present invention with regard to issuing, managing and redeeming electronic tickets or other stored-value data objects within the realm of e-commerce or in the context of other types of secure transactions, it should be understood that the exemplary details above are not limiting.

Claims

1. A system (10) to securely manage stored-value data objects, the system comprising:

   an issuing system (12) to issue a stored-value data object to a user device (16), wherein the issuing system signs the stored-value data object and encrypts the stored-value data object using a first public key (PTD_{PuK}) associated with the user device;
   a security element (20) comprising a portion of the user device (16) to decrypt and securely store the stored-value data object received at the user device from the issuing system (12); and
   a redeeming system (14) to redeem the stored-value data object by receiving the stored-value data object from the user device;

   characterized in that the security element (20) encrypts the stored-value data object with a second public key (TRS_{PuK}) received from the redeeming system and associated with the redeeming system (14);
   and wherein the redeeming system (14) decrypts the stored-value data object and verifies that the stored-value data object was signed by the issuing system (12).

2. The system of claim 1, wherein the security element (20) comprises a memory device (62) providing non-volatile storage for a first private key (PTD_{PrK}) corresponding to the first public key used by the issuing system (12) to encrypt the stored-value data object.

3. The system of claim 1, wherein the issuing system (12) comprises:

   a communication interface (70) to receive stored-value data object requests and issue stored-value data objects;
   a processing system (72) to sign and encrypt stored-value data objects; and
   memory (74) to store an issuing system private key (TIS_{PrK}) used in signing stored-value data objects.

4. The system of claim 1, wherein the redeeming system (14) comprises:

   a communication interface (80) to receive re-

demption requests and stored-value data objects from user devices;
a processing system (82) to decrypt and verify stored-value data objects received from user devices; and
memory (84) to store a redeeming system private key (TRS_{PrK}) used in decrypting the received stored-value data objects.

5. The system of claim 1 further comprising a second redeeming system (14) to verify a multi-use stored-value data object returned to the user device (16) from the first redeeming system (14) responsive to the user device redeeming the stored-value data object received from the ticket issuing system (12).

6. The system of claim 1 further comprising a rapid verification system (100) to redeem a rapid verification token (RVT) generated by the security element (20) in the user device (16), and wherein the redeeming system (14) is arranged to return a seed value to the user device responsive to the user device redeeming the stored-value data object at the redeeming system, the said seed value determining at least one pseudorandom element of the said RVT.

7. A user device (16) serving as a secure agent for stored-value data object issuing (12) and redeeming (14) systems, the user device comprising:

at least one wireless interface (42, 44) to communicate with the issuing and redeeming systems; and
a security element (20) comprising at least one processor (60) and associated memory (62) to:

securely store a first private key (PTD_{PrK}) associated with the security element;
decrypt a stored-value data object received from the issuing system (12) using the first private key (PTD_{PrK}) and securely store the decrypted stored-value data object;

characterized in that the security element (20) is further arranged to:

encrypt the stored-value data object and a generated value using a second public key (TRS_{PuK}) associated with the redeeming system (14), wherein the
second public key (TRS_{PuK}) and the generated value are received from the redeeming system (14);
transfer the encrypted stored-value data object and generated value to the redeeming system (14); and
erase the stored-value data object from the associated memory (62)in the security element (20) responsive to transfer of stored-value data object to the redeeming system (14).

8. The user device of claim 7, wherein the at least one wireless interface (42, 44) comprises first and second wireless interfaces and wherein the second wireless interface (44) is a local wireless interface, and further wherein the redeeming system (14) is local with respect to the user device (16), such that the security element (20) and the redeeming system (14) communicate via the second wireless interface (44).

9. The user device of claim 7, wherein the security element (20) receives a modified stored-value data object from the redeeming system (14) responsive to redeeming the stored-value data object, if the stored-value data object was a multi-use stored-value data object.

10. The user device of claim 7, wherein the security element (20) further comprises a sequence/pattern generator (64) to generate at least one pseudorandom element as part of rapid verification activities subsequent to redeeming the stored-value data object at the redeeming system (14).

11. A method of securely managing the issuance and redemption of stored-value data objects, the method comprising:

issuing a stored-value data object from an issuing system (12) to a user device (16), wherein the issuing system encrypts the stored-value data object using a first public key (PTD_{PuK}) associated with the user device and the user device (16) decrypts the stored-value data object using a private key (PTD_{PrK}) known to the user device;

characterized by the method further comprising:

transferring a second public key (TRS_{PuK}) received from a redeeming system (14) and associated with the redeeming system to the user device (16) responsive to a redemption request;
receiving the stored-value data object from the user device (16) at the redeeming system (14), wherein the stored-value data object is encrypted by the user device (16) using the second public key (TRS_{PuK}); and
validating the stored-value data object at the redeeming system (14) after decrypting the stored-value data object using a private key (TRS_{PrK}) known to the redeeming system (14).

12. The method of claim 11 further comprising transferring a generated value from the redeeming system (14) to the user device (16) responsive to the redemption request.

13. The method of claim 12, wherein the user device (16) uses both the generated value and the second public key (TRS_{PuK}) to encrypt the stored-value data object received at the redeeming system (14), and wherein the redeeming system validates both the stored-value data object and the generated value after decrypting the stored-value data object and the generated value using private key (TRS_{PrK}) known to the redeeming system (14).

14. The method of claim 13, wherein validating the generated value and the stored-value data object returned from the user device (16) to the redeeming system (14) comprises verifying that the generated value returned from the user device matches the generated value sent from the redeeming system to the user device.

15. The method of claim 13, wherein validating the generated value and the stored-value data object returned from the user device (16) to the redeeming system (14) comprises verifying that the stored-value data object is signed by the issuing system (12).

16. The method of claim 15, wherein verifying that the stored-valued data object is signed by the issuing system (12) comprises validating a digital signature using a second private key at the redeeming system (14), and wherein the second private key is associated with the issuing system (12).

17. The method of claim 15, wherein verifying that the stored-valued data object is signed by the issuing system (12) comprises validating a digital signature using a second private key at the redeeming system (14), and wherein the second private key is associated with another redeeming system.

18. The method of claim 12 or 13 further comprising generating the generated value as a nonce.

19. The method of claim 11 further comprising configuring the issuing system (12) as a WAP-enabled server, which is also capable of generating and responding to special ticketing MIME types, allowing the user device (16) to request and receive the stored-value data object in accordance with WAP procedures complemented with the said MIME types.

20. The method of claim 11 further comprising returning a modified stored-value data object from the redeeming system (14) to the user device (16) if the stored-value data object being redeemed by the user device (16) is a multi-use stored-value data object.

21. The method of claim 20 further comprising modifying the multi-use stored-value data object received at the redeeming system (14) from the user device (16) by setting a redemption counter value in the multi-use stored-value data object, wherein the redemption counter value comprises a portion of the data comprising the stored-value data object.

22. The method of claim 13 further comprising returning a seed value to the user device (16) if the generated value and stored-value data object received from the user device (16) are validated.

23. The method of claim 22 further comprising:

receiving a verification sequence including a first pseudorandom element at a rapid verification system (100);
validating the verification sequence by determining whether the first pseudorandom element matches a second pseudorandom element generated by the verification system using the same seed value; and
wherein the user device (16) generates the first pseudorandom element using the seed value received from the redeeming system (14).

24. The method of claim 22 further comprising verifying by a human operator at a rapid verification point a verification image generated by the user device (16), wherein the verification image is dependent on the seed value returned to the user device (16) by the redeeming system (14).

25. The method of claim 11 further comprising receiving the first public key (PTD_{PuK}) at the redeeming system (14).

26. The method of claim 25 further comprising returning a redeemed stored-value data object encrypted using the first public key (PTD_{PuK}) to the user device (16) from the redeeming system (14).

27. The method of claim 26 further comprising exchanging the redeemed stored-value data object for a temporary stored-value data object that may be subsequently validated on a temporary basis.

28. The method of claim 25 further comprising returning a seed value, encrypted using the first public key (PTD_{PuK}) associated with the user device (16), from the redeeming system (14) to the user device (16).

29. The method of claim 28 further comprising verifying the temporary stored-value data object, based on the seed value, during a subsequent redemption attempt by the user device (16).

30. The method of claim 29, wherein verifying the temporary stored-value data object, based on the seed value, during a subsequent redemption attempt by

the user device (16) comprises verifying a pseudorandom number sequence returned from the user device (16) based on the seed value and a redemption-system time-of-day value.

31. The method of claim 27 further comprising verifying the temporary stored-value data object at a second redeeming system (14) using a reduced-security redemption protocol as compared to the initial verification of the stored-value data object at the first redeeming system (14).

Patentansprüche

1. System (10) für die sichere Handhabung von gespeicherten Wertdatenobjekten, wobei das System aufweist:

ein Ausgabesystem (12) zur Ausgabe eines gespeicherten Wertdatenobjektes an eine Benutzervorrichtung (16), wobei das Ausgabesystem das gespeicherte Wertdatenobjekt signiert und das gespeicherte Wertdatenobjekt unter Verwendung eines ersten allgemeinen Schlüssels (PTD_{PuK}), welche der Benutzervorrichtung zugeordnet ist, verschlüsselt;
ein Sicherheitselement (20), umfassend einen Bereich in der Benutzervorrichtung (16) zum Entschlüsseln und zum sicheren Speichern des gespeicherten Wertdatenobjektes, das an der Benutzervorrichtung von dem Ausgabesystem (12) empfangen wurde; und
ein Lösesystem (14) zum Lösen des gespeicherten Wertdatenobjektes, indem das gespeicherte Wertdatenobjekt von der Benutzervorrichtung empfangen wird;

dadurch gekennzeichnet, dass das Sicherheitselement (20) das gespeicherte Wertdatenobjekt mit einem zweiten allgemeinen Schlüssel (TRS_{PuK}), der von dem Lösesystem (14) empfangen wird und dem Lösesystem (14) zugeordnet ist, verschlüsselt;
und wobei das Lösesystem (14) das gespeicherte Wertdatenobjekt entschlüsselt und verifiziert, dass das gespeicherte Wertdatenobjekt von dem Ausgabesystem (12) signiert wurde.

2. System nach Anspruch 1, wobei das Sicherheitselement (20) eine Speichervorrichtung (62) umfasst, die ein nicht-flüchtiges Speichern eines ersten persönlichen Schlüssels (PTD_{PrK}), der dem ersten allgemeinen Schlüssel entspricht, der von dem Ausgabesystem (12) verwendet wird, ermöglicht, um das gespeicherte Datenobjekt zu verschlüsseln.

3. System nach Anspruch 1; wobei das Ausgabesystem (12) umfasst:

eine Kommunikationsschnittstelle (70) zum Empfangen von Anfragen nach gespeicherten Wertdatenobjekten und zum Ausgeben von gespeicherten Wertdatenobjekten;
ein Verarbeitungssystem (72) zum Signieren und Verschlüsseln von gespeicherten Wertdatenobjekten; und
einen Speicher (74) zum Speichern eines persönlichen Ausgabesystemschlüssels (TIS_{PrK}), der zum Signieren von gespeicherten Wertdatenobjekten verwendet wird.

4. System nach Anspruch 1, wobei das Lösesystem (14) aufweist:

eine Kommunikationsschnittstelle (18) zum Empfangen von Löseanfragen und von gespeicherten Wertdatenobjekten von Benutzervorrichtungen;
ein Verarbeitungssystem (82) zum Entschlüsseln und Verifizieren von gespeicherten Wertdatenobjekten, die von Benutzereinrichtungen empfangen wurden; und
einen Speicher (84) zum Speichern eines persönlichen Lösesystemschlüssels (TRS_{PrK}), der zum Entschlüsseln der empfangenen, gespeicherten Wertdatenobjekte verwendet wird.

5. System nach Anspruch 1, das ferner ein zweites Lösesystem (14) aufweist, um ein gespeichertes Mehrzweck-Wertdatenobjekt zu verifizieren, das zu der Benutzervorrichtung (16) von dem ersten Lösesystem (14) als Antwort auf das Lösen des gespeicherten Wertdatenobjektes, das von dem ersten Ticketausgabesystem (12) empfangen wurde, durch die Benutzervorrichtung zurückgesendet wurde.

6. System nach Anspruch 1, das ferner ein Schnellverifizierungssystem (100) aufweist, um ein Schnellverifizierungsmittel (RVT), das durch das Sicherheitselement (20) in der Benutzervorrichtung (16) erzeugt wurde, zu lösen, und wobei das Lösesystem (14) angeordnet ist, um einen Seed-Wert an die Benutzervorrichtung als Antwort auf das Lösen des gespeicherten Wertdatenobjektes an dem Lösesystem durch die Benutzervorrichtung zurückzusenden, wobei der Seed-Wert wenigstens ein pseudo-zufälliges Element des RVT bestimmt.

7. Benutzervorrichtung (16), die als ein Sicherheitsmittel für Systeme zur Ausgabe (12) und zum Lösen (14) von gespeicherten Wertdatenobjekten dient, wobei die Benutzervorrichtung aufweist:

wenigstens eine drahtlose Schnittstelle (42, 44), um mit den Ausgabe- und Lösesystemen zu kommunizieren; und
ein Sicherheitselement (20), das wenigstens ei-

nen Prozessor (60) und einen zugeordneten Speicher (62) aufweist, um:

einen ersten persönlichen Schlüssel (PTD_{PrK}), der dem Sicherheitselement zugeordnet ist, sicher zu speichern;
ein gespeichertes Wertdatenobjekt, das von dem Ausgabesystem (12) empfangen wird, unter Verwendung des ersten persönlichen Schlüssels (PTD_{PrK}) zu entschlüsseln; und um das entschlüsselte, gespeicherte Wertdatenobjekt sicher zu speichern;

dadurch gekennzeichnet, dass das Sicherheitselement (20) ferner angeordnet ist, um:

das gespeicherte Wertdatenobjekt und einen erzeugten Wert unter Verwendung eines zweiten allgemeinen Schlüssels (TRS_{PuK}), der dem Lösesystem (14) zugeordnet ist, zu entschlüsseln, wobei der zweite allgemeine Schlüssel (TRS_{PuK}) und der zweite Wert von dem Lösesystem (14) empfangen werden;
das verschlüsselte, gespeicherte Wertdatenobjekt und den erzeugten Wert zu dem Lösesystem (14) zu transferieren; und
das gespeicherte Wertdatenobjekt aus dem zugeordneten Speicher (62) in dem Sicherheitselement (20) als Antwort auf den Transfer des gespeicherten Wertdatenobjektes zu dem Lösesystem (14) zu löschen.

8. Benutzervorrichtung nach Anspruch 7, wobei die wenigstens eine drahtlose Schnittstelle (42, 44) erste und zweite drahtlose Schnittstellen umfasst, und wobei die zweite drahtlose Schnittstelle (44) eine lokale drahtlose Schnittstelle ist, und wobei ferner das Lösesystem (14) in Bezug auf die Benutzervorrichtung (16) lokal ist, so dass das Sicherheitselement (20) und das Lösesystem (14) über die zweite drahtlose Schnittstelle (44) miteinander kommunizieren.

9. Benutzervorrichtung nach Anspruch 7, wobei das Sicherheitselement (20) ein modifiziertes, gespeichertes Wertdatenobjekt von dem Lösesystem (14) als Antwort auf das Lösen des gespeicherten Wertdatenobjektes empfängt, wenn das gespeicherte Wertdatenobjekt ein gespeichertes Mehrzweck-Wertdatenobjekt war.

10. Benutzervorrichtung nach Anspruch 7, wobei das Sicherheitselement (20) ferner einen Sequenz/Mustergenerator (64) umfasst, um wenigstens ein pseudo-zufälliges Element als ein Teil der Schnellverifizierungsaktivitäten folgend auf das Lösen des gespeicherten Wertdatenobjektes an dem Lösesystem (14) zu erzeugen.

11. Verfahren zum sicheren Handhaben der Ausgabe und des Lösens von gespeicherten Wertdatenobjekten, wobei das Verfahren die Schritte aufweist:

Ausgeben eines gespeicherten Wertdatenobjektes von einem Ausgabesystem (12) an eine Benutzervorrichtung (16), wobei das Ausgabesystem das gespeicherte Wertdatenobjekt unter Verwendung eines ersten allgemeinen Schlüssels (PTD_{PuK}), welcher der Benutzervorrichtung zugeordnet ist, verschlüsselt, und die Benutzervorrichtung (16) das gespeicherte Wertdatenobjekt unter Verwendung eines persönlichen Schlüssels (PTD_{PrK}), welcher der Benutzervorrichtung bekannt ist, entschlüsselt;

dadurch gekennzeichnet, dass das Verfahren ferner die Schritte aufweist:

Transferieren eines zweiten allgemeinen Schlüssels (TRS_{PuK}), der von einem Lösesystem (14) empfangen wurde und dem Lösesystem zugeordnet ist, an die Benutzervorrichtung (16) als Antwort auf eine Löseanfrage;
Empfangen des gespeicherten Wertdatenobjektes von der Benutzervorrichtung (16) an dem Lösesystem (14), wobei das gespeicherte Wertdatenobjekt durch die Benutzervorrichtung (16) unter Verwendung des zweiten allgemeinen Schlüssels (TRS_{PuK}) verschlüsselt wird; und
Validieren des gespeicherten Wertdatenobjektes an dem Lösesystem (14) nach dem Entschlüsseln des gespeicherten Wertdatenobjektes unter Verwendung eines persönlichen Schlüssels (TRS_{PrK}), der dem Lösesystem (14) bekannt ist.

12. Verfahren nach Anspruch 11, das ferner das Transferieren eines erzeugten Wertes von dem Lösesystem (14) zu der Benutzervorrichtung (16) als Antwort auf die Löseanfrage transferiert.

13. Verfahren nach Anspruch 12, wobei die Benutzervorrichtung (16) sowohl den generierten Wert als auch den zweiten allgemeinen Schlüssel (TRS_{PuK}) zum Verschlüsseln des gespeicherten Wertdatenobjektes verwendet, das an dem Lösesystem (14) empfangen wurde, und wobei das Lösesystem sowohl das gespeicherte Wertdatenobjekt als auch den generierten Wert nach dem Entschlüsseln des gespeicherten Wertdatenobjektes und des generierten Wertes unter Verwendung eines persönlichen Schlüssels (TRS_{PrK}), der dem Lösesystem (14) bekannt ist, validiert.

14. Verfahren nach Anspruch 13, wobei das Validieren des generierten Wertes und des gespeicherten Wertdatenobjektes, das von der Benutzervorrich-

tung (16) an das Lösesystem (14) zurückgesendet wurde, das Verifizieren umfasst, dass der generierte Wert, der von der Henutzervorrichtung zurückgesendet wurde, mit dem generierten Wert, der von dem Lösesystem zu der Benutzervorrichtung gesendet wurde, übereinstimmt.

15. Verfahren nach Anspruch 13, wobei das validieren des generierten Wertes und des gespeicherten Wertdatenobjektes, das von der Benutzervorrichtung (16) zu dem Lösesystem (14) zurückgesendet wurde, das Verifizieren aufweist, dass das gespeicherte Wertdatenobjekt durch das Ausgabesystem (12) signiert wurde.

16. Verfahren nach Anspruch 15, wobei das Verifizieren, dass das gespeicherte Wertdatenobjekt durch das Ausgabesystem (12) signiert ist, das Validieren einer digitalen Signatur unter Verwendung eines zweiten persönlichen Schlüssels an dem Lösesystem (14) aufweist, und wobei der zweite persönliche Schlüssel dem Ausgabesystem (12) zugeordnet ist.

17. Verfahren nach Anspruch 15, wobei das Verifizieren, dass das gespeicherte Wertdatenobjekt durch das Ausgabesystem (12) signiert ist, das Validieren einer digitalen Signatur unter Verwendung eines zweiten persönlichen Schlüssels an dem Lösesystem (14) aufweist, und wobei der zweite persönliche Schlüssel dem anderen Lösesystem zugeordnet ist.

18. Verfahren nach Anspruch 12 oder 13, das ferner das Generieren des generierten Wertes als eine Nonce umfasst.

19. Verfahren nach Anspruch 11, das ferner das Konfigurieren des Ausgabesystems (12) als ein WAP-aktiver Server aufweist, der auch zum Generieren und Antworten auf spezielle Ticketing-MIME-Arten geeignet ist, so dass es der Benutzervorrichtung (16) möglich ist, das gespeicherte Wertdatenobjekt in Übereinstimmung mit WAP-Verfahren, die mit den MIME-Arten ergänzt werden, abzufragen und zu empfangen.

20. Verfahren nach Anspruch 11, das ferner das Zurücksenden eines modifizierten, gespeicherten Wertdatenobjektes von dem Lösesystem (14) an die Benutzervorrichtung (16) aufweist, wenn das gespeicherte Wertdatenobjekt, das von der Benutzervorrichtung (16) gelöst wird, ein gespeichertes Mehrzweck-Wertdatenobjekt ist.

21. Verfahren nach Anspruch 20, das ferner das Modifizieren des gespeicherten Mehrzweck-Wertdatenobjektes, das an dem Lösesystem (14) von der Benutzervorrichtung (16) empfangen wurde, aufweist, indem ein Löse-Zählwert in dem gespeicherten Mehrzweck-Wertdatenobjekt gesetzt wird, wobei der Löse-Zählwert einen Bereich der Daten aufweist, die das gespeicherte Wertdatenobjekt umfassen.

22. Verfahren nach Anspruch 13, dass ferner das Zurücksenden eines Seed-Wertes an die Benutzervorrichtung (16) aufweist, wenn der generierte Wert und das gespeicherte Wertdatenobjekt, das von der Benutzervorrichtung (16) empfangen wurde, validiert sind.

23. Verfahren nach Anspruch 22, das ferner die Schritte aufweist:

Empfangen einer Verifizierungssequenz, die ein erstes pseudo-zufälliges Element aufweist, an einem Schnellverifizierungssystem (100);
Validieren der Verifizierungssequenz, indem bestimmt wird, ob das erste pseudo-zufällige Element mit einem zweiten pseudo-zufälligen Element, das durch das Verifizierungssystem unter Verwendung desselben Seed-Wertes generiert wurde, übereinstimmt; und
wobei die Benutzervorrichtung (16) das erste pseudo-zufällige Element unter Verwendung des Seed-Wertes erzeugt, der von dem Lösesystem (14) empfangen wurde.

24. Verfahren nach Anspruch 22, das ferner das Verifizieren eines durch die Benutzervorrichtung (16) generierten Verifizierungsbildes durch einen menschlichen Operator an einem Schnellverifizierungspunkt aufweist, wobei das Verifizierungsbild von dem Seed-Wert, der zu der Benutzervorrichtung (16) durch das Lösesystem (14) zurückgesendet wurde, abhängig ist.

25. Verfahren nach Anspruch 11, das ferner das Empfangen des ersten allgemeinen Schlüssels (PTD_{PuK}) an dem Lösesystem (14) aufweist.

26. Verfahren nach Anspruch 25, das ferner das zurücksenden eines gelösten, gespeicherten Wertdatenobjektes, das unter Verwendung des ersten allgemeinen Schlüssels (PTD_{PuK}) verschlüsselt wurde, an die Benutzervorrichtung (16) von dem Lösesystem (14) aufweist.

27. Verfahren nach Anspruch 26, das ferner das Austauschen des gelösten, gespeicherten Wertdatenobjektes durch ein temporär gespeichertes Wertdatenobjekt aufweist, das anschließend auf einer temporären Basis validiert werden kann.

28. Verfahren nach Anspruch 25, das ferner das Zurücksenden eines Seed-Wertes, der unter Verwendung des ersten allgemeinen Schlüssels (PTD_{PuK}), welche der Benutzervorrichtung (16) zugeordnet ist,

verschlüsselt wurde, von dem Lösesystem (14) zu der Benutzervorrichtung (16) aufweist.

29. Verfahren nach Anspruch 28, das ferner das Verifizieren des temporär gespeicherten Wertdatenobjektes, das auf dem Seed-Wert basiert, während eines darauf folgenden Löseversuchs durch die Benutzervorrichtung (16) aufweist.

30. Verfahren nach Anspruch 29, wobei das Verifizieren des temporär gespeicherten Wertdatenobjektes, das auf dem Seed-Wert basiert, während eines darauf folgenden Löseversuchs durch die Benutzervorrichtung (16) das Verifizieren einer pseudo-zufälligen Laufnummer, die von der Benutzervorrichtung (16) basierend auf dem Seed-Wert und einem Löse-System-Tageszeitwert zurückgesendet wurde, aufweist.

31. Verfahren nach Anspruch 27, das ferner das Verifizieren des temporär gespeicherten Wertdatenohjektes an einem zweiten Lösesystem (14) unter Verwendung eines Löseprotokolls mit reduzierter Sicherheit, verglichen mit der Anfangsverifizierung des gespeicherten Wertdatenobjektes an dem ersten Lösesystem (14) aufweist.

Revendications

1. système (10) pour gérer de manière sécurisée des objets de données à valeur stockée, le système comprenant :

> un système de délivrance (12) pour délivrer un objet à valeur stockée à un dispositif d'utilisateur (16), dans lequel le système de délivrance signe l'objet de données à valeur stockée et chiffre l'objet de données à valeur stockée en utilisant une première clé publique (PTD_{PuK}) associée au dispositif d'utilisateur;
> un élément de sécurité (20) comprenant une partie du dispositif d'utilisateur (16) pour déchiffrer et stocker de manière sécurisée l'objet de données à valeur stockée reçu au dispositif d'utilisateur à partir du système de délivrance (12); et un système de rachat (14) pour racheter l'objet de données à valeur stockée en recevant l'objet de données à valeur stockée à partir du dispositif d'utilisateur;

caractérisé en ce que l'élément de sécurité (20) chiffre l'objet de données à valeur stockée avec une seconde clé publique (TRS_{PuK}) reçue du système de rachat et associée au système de rachat (14);
et le système de rachat (14) déchiffre l'objet de données à valeur stockée et vérifie que l'objet de données à valeur stockée a été signé par le système de délivrance (12).

2. Système selon la revendication 1, dans lequel l'élément de sécurité (20) comprend un dispositif de mémoire (62) procurant un stockage non volatil pour une première clé privée (PTD_{PrK}) correspondant à la première clé publique utilisée par le système de délivrance (12) pour chiffrer l'objet de données à valeur stockée.

3. Système selon la revendication 1, dans lequel le système de délivrance (12) comprend :

> une interface de communication (70) pour recevoir des demandes d'objets de données à valeur stockée et pour délivrer des objets de données à valeur stockée;
> un système de traitement (72) pour signer et chiffrer des objets de données à valeur stockée; et
> une mémoire (74) pour stocker une clé privée de système de délivrance (TIS_{PrK}) utilisée pour signer des objets de données à valeur stockée.

4. Système selon la revendication 1, dans lequel le système de rachat (14) comprend :

> une interface de communication (80) pour recevoir des demandes de rachat et des objets de données à valeur stockée provenant de dispositifs d'utilisateur;
> un système de traitement (82) pour déchiffrer et vérifier des objets de données à valeur stockée reçus de dispositifs d'utilisateur; et
> une mémoire (84) pour stocker une clé privée de système de rachat (TRS_{PrK}) utilisée dans le déchiffrement des objets de données à valeur stockée reçus.

5. Système selon la revendication 1, comprenant en outre un second système de rachat (14) pour vérifier un objet de données à valeur stockée multi-usage retourné vers le dispositif d'utilisateur (16) à partir du premier système de rachat (14) en réponse à la restitution par le dispositif d'utilisateur de l'objet de données à valeur stockée reçu du système de délivrance de tickets (12).

6. Système selon la revendication 1, comprenant en outre un système de vérification rapide (100) pour racheter un jeton de vérification rapide (RVT) généré par l'élément de sécurité (20) dans le dispositif d'utilisateur (16), et dans lequel le système de rachat (14) est agencé pour retourner une valeur de graine au dispositif d'utilisateur en réponse à la restitution par le dispositif d'utilisateur de l'objet de données à valeur stockée, au système de rachat, ladite valeur de graine déterminant au moins un élément pseudo-

aléatoire dudit RVT.

7. Dispositif d'utilisateur (16) remplissant la fonction d'un agent sécurisé pour des systèmes de délivrance (12) et de rachat (14) d'objets de données à valeur stockée, le dispositif d'utilisateur comprenant :

au moins une interface sans fil (42, 44) pour communiquer avec les systèmes de délivrance et de rachat; et
un élément de sécurité (20) comprenant au moins un processeur (60) et une mémoire (62) associée pour :

stocker de manière sécurisée une première clé privée (PTD_{PrK}) associée à l'élément de sécurité;
déchiffrer un objet de données à valeur stockée reçu du système de délivrance (12), en utilisant la première clé privée (PTD_{PrK}), et stocker de manière sécurisée l'objet de données à valeur stockée déchiffré;

caractérisé en ce que l'élément de sécurité (20) est en outre agencé pour :

chiffrer l'objet de données à valeur stockée et une valeur générée en utilisant une seconde clé publique (TRS_{PuK}) associée au système de rachat (14), la seconde clé publique (TRS_{PuK}) et la valeur générée étant reçues du système de rachat (14);
transférer vers le système de rachat (14) l'objet de données à valeur stockée et la valeur générée chiffrés; et
effacer l'objet de données à valeur stockée de la mémoire (62) associée dans l'élément de sécurité (20), en réponse au transfert de l'objet de données à valeur stockée vers le système de rachat (14).

8. Dispositif d'utilisateur selon la revendication 7, dans lequel l'au moins une interface sans fil (42, 44) comprend des première et seconde interfaces sans fil, et dans lequel la seconde interface sans fil (44) est une interface sans fil locale, et en outre dans lequel le système de rachat (14) est local vis-à-vis du dispositif d'utilisateur (16), de façon que l'élément de sécurité (20) et le système de rachat (14) communiquent par l'intermédiaire de la seconde interface sans fil (44).

9. Dispositif d'utilisateur selon la revendication 7, dans lequel l'élément de sécurité (20) reçoit un objet de données à valeur stockée modifié provenant du système de rachat (14), en réponse au rachat de l'objet de données à valeur stockée, si l'objet de données à valeur stockée était un objet de données à valeur stockée multi-usage.

10. Dispositif d'utilisateur selon la revendication 7, dans lequel l'élément de sécurité (20) comprend en outre un générateur de séquence / configuration (64) pour générer au moins un élément pseudo-aléatoire dans le cadre d'activités de vérification rapide à la suite du rachat de l'objet de données à valeur stockée au système de rachat (14).

11. Procédé pour gérer de manière sécurisée la délivrance et le rachat d'objets de données à valeur stockée, le procédé comprenant :

la délivrance à un dispositif d'utilisateur (16) d'un objet de données à valeur stockée provenant d'un système de délivrance (12), le système de délivrance chiffrant l'objet de données à valeur stockée en utilisant une première clé publique (PTD_{PuK}) associée au dispositif d'utilisateur, et le dispositif d'utilisateur (16) déchiffrant l'objet de données à valeur stockée en utilisant une clé privée (PTD_{PrK}) connue du dispositif d'utilisateur;

caractérisé en ce que le procédé comprend en outre:

le transfert vers le dispositif d'utilisateur (16) d'une seconde clé publique (TRS_{PuK}) reçue d'un système de rachat (14) et associée au système de rachat, en réponse à une demande de rachat;
la réception au système de rachat (14) de l'objet de données à valeur stockée provenant du dispositif d'utilisateur (16), l'objet de données à valeur stockée étant chiffré par le dispositif d'utilisateur (16) en utilisant la seconde clé publique (TRS_{PuK}); et
la validation de l'objet de données à valeur stockée, au système de rachat (14), après le déchiffrement de l'objet de données à valeur stockée en utilisant une clé privée (TRS_{PrK}) connue du système de rachat (14).

12. Procédé selon la revendication 11, comprenant en outre le transfert vers le dispositif d'utilisateur (16) d'une valeur générée provenant du système de rachat (14), en réponse à la demande de rachat.

13. Procédé selon la revendication 12, dans lequel le dispositif d'utilisateur (16) utilise à la fois la valeur générée et la seconde clé publique (TRS_{PuK}) pour chiffrer l'objet de données à valeur stockée reçu au système de rachat (14), et dans lequel le système de rachat valide à la fois l'objet de données à valeurs stockée et la valeur générée après avoir déchiffré l'objet de données à valeur stockée et la valeur gé-

nérée en utilisant une clé privée (TRS_{PrK}) connue du système de rachat (14).

14. Procédé selon la revendication 13, dans lequel la validation de la valeur générée et de l'objet de données à valeur stockée retournés du dispositif d'utilisateur (16) au système de rachat (14) comprend la vérification du fait que la valeur générée retournée du dispositif d'utilisateur concorde avec la valeur générée envoyée du système de rachat au dispositif d'utilisateur.

15. Procédé selon 1a revendication 13, dans lequel la validation de la valeur générée et de l'objet de données à valeur stockée retournés du dispositif d'utilisateur (16) au système de rachat (14) comprend la vérification du fait que l'objet de données à valeur stockée est signé par le système de délivrance (12).

16. Procédé selon la revendication 15, dans lequel la vérification du fait que l'objet de données à valeur stockée est signé par le système de délivrance (12) comprend la validation d'une signature numérique en utilisant une seconde clé privée au système de rachat (14), et dans lequel la seconde clé privée est associée au système de délivrance (12).

17. Procédé selon la revendication 15, dans lequel la vérification du fait que l'objet de données à valeur stockée est signé par le système de délivrance (12) comprend la validation d'une signature numérique en utilisant une seconde clé privée au système de rachat (14), et dans lequel la seconde clé privée est associée à un autre système de rachat.

18. Procédé selon la revendication 12 ou 13, comprenant en outre la génération de la valeur générée comme une valeur prévue pour une utilisation unique.

19. Procédé selon la revendication 11, comprenant en outre la configuration du système de délivrance (12) comme un serveur ayant une capacité WAP, qui est également capable de générer des types MIME spéciaux pour l'émission de tickets, ainsi que de réagir à ces types, permettant au dispositif d'utilisateur (16) de demander et de recevoir l'objet de données à valeur stockée conformément à des procédures WAP complétées par lesdits types MIME.

20. Procédé selon la revendication 11, comprenant en outre le retour d'un objet de données à valeur stockée modifié, du système de rachat (14) vers le dispositif d'utilisateur (16), si l'objet de données à valeur stockée dont le rachat est demandé par le dispositif d'utilisateur (16) est un objet de données à valeur stockée multi-usage.

21. Procédé selon la revendication 20, comprenant en outre la modification de l'objet de données à valeur stockée multi-usage reçu au système de rachat (14) à partir du dispositif d'utilisateur (16), en fixant une valeur de compteur de rachat dans l'objet de données à valeur stockée multi-usage, dans lequel la valeur de compteur de rachat comprend une partie des données constituant l'objet de données à valeur stockée.

22. Procédé selon la revendication 13, comprenant en outre le retour d'une valeur de graine au dispositif d'utilisateur (16) si la valeur générée et l'objet de données à valeur stockée reçus du dispositif d'utilisateur (16) sont validés.

23. Procédé selon la revendication 22, comprenant en outre les étapes suivantes :

recevoir à un système de vérification rapide (100) une séquence de vérification incluant un premier élément pseudo-aléatoire;
valider la séquence de vérification en déterminant si le premier élément pseudo-aléatoire concorde avec un second élément pseudo-aléatoire généré par le système de vérification en utilisant la même valeur de graine; et
dans lequel le dispositif d'utilisateur (16) génère le premier élément pseudo-aléatoire en utilisant la valeur de graine reçue du système de rachat (14).

24. Procédé selon la revendication 22, comprenant en outre la vérification par un opérateur humain, à un point de vérification rapide, d'une image de vérification générée par le dispositif d'utilisateur (16), dans lequel l'image de vérification dépend de la valeur de graine retournée au dispositif d'utilisateur (16) par le système de rachat (14).

25. Procédé selon la revendication 11, comprenant en outre la réception de la première clé publique (PTD_{PuK}) au système de rachat (14).

26. Procédé selon la revendication 25, comprenant en outre le retour au dispositif d'utilisateur (16), à partir du système de rachat (14), d'un objet de données à valeur stockée racheté, chiffré en utilisant la première clé publique (PTD_{PuK})

27. Procédé selon la revendication 26, comprenant en outre l'échange de l'objet de données à valeur stockée racheté contre un objet de données à valeur stockée temporaire qui peut ensuite être validé sur une base temporaire.

28. Procédé selon la revendication 25, comprenant en outre le retour au dispositif d'utilisateur (16), à partir

du système de rachat (14), d'une valeur de graine chiffrée en utilisant la première clé publique (PTD_{PuK}) associée au dispositif d'utilisateur (16).

29. Procédé selon la revendication 28, comprenant en outre la vérification de l'objet de données à valeur stockée temporaire, sur la base de la valeur de graine, pendant une tentative de rachat ultérieure effectuée par le dispositif d'utilisateur (16).

30. Procédé selon la revendication 29, dans lequel la vérification de l'objet de données à valeur stockée temporaire, sur la base de la valeur de graine, pendant une tentative de rachat ultérieure effectuée par le dispositif d'utilisateur (16), comprend la vérification d'une séquence de nombres pseudo-aléatoire retournée à partir du dispositif d'utilisateur (16), basée sur la valeur de graine et sur une valeur de l'heure courante du système de rachat.

31. Procédé selon la revendication 27, comprenant en outre la vérification de l'objet de données à valeur stockée temporaire à un second système de rachat (14) en utilisant un protocole de rachat à sécurité réduite en comparaison avec la vérification initiale de l'objet de données à valeur stockée au premier système de rachat (14).

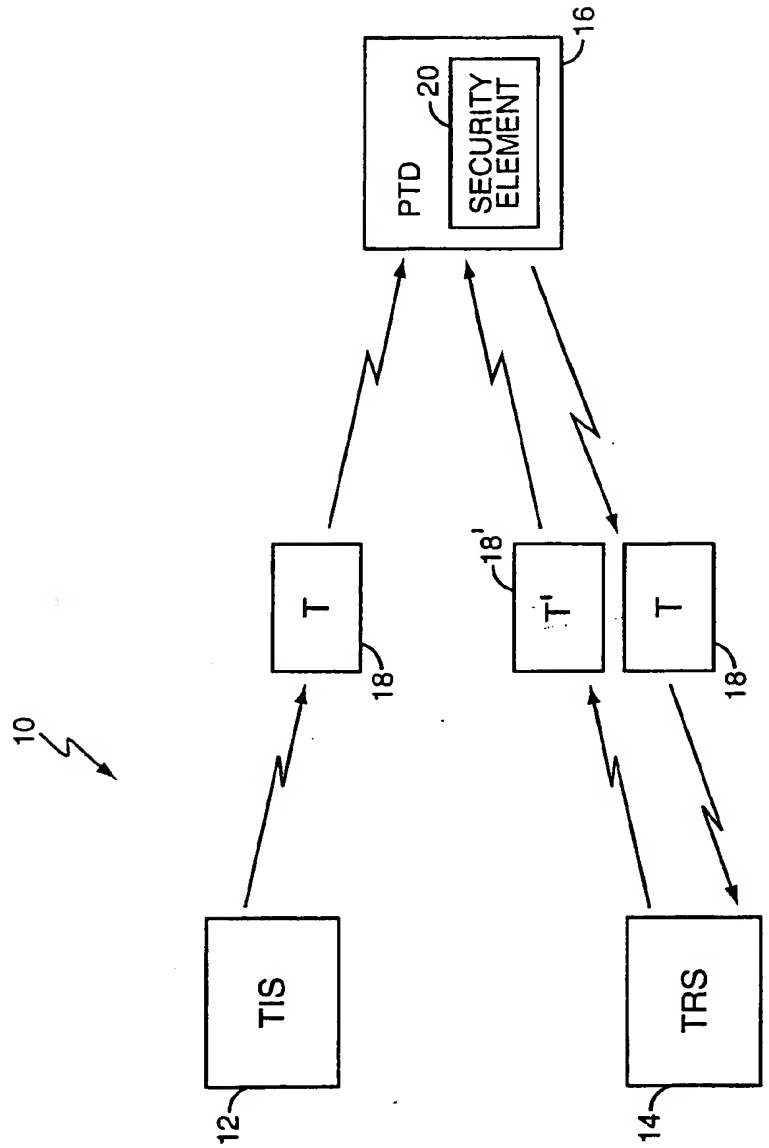

FIG. 1

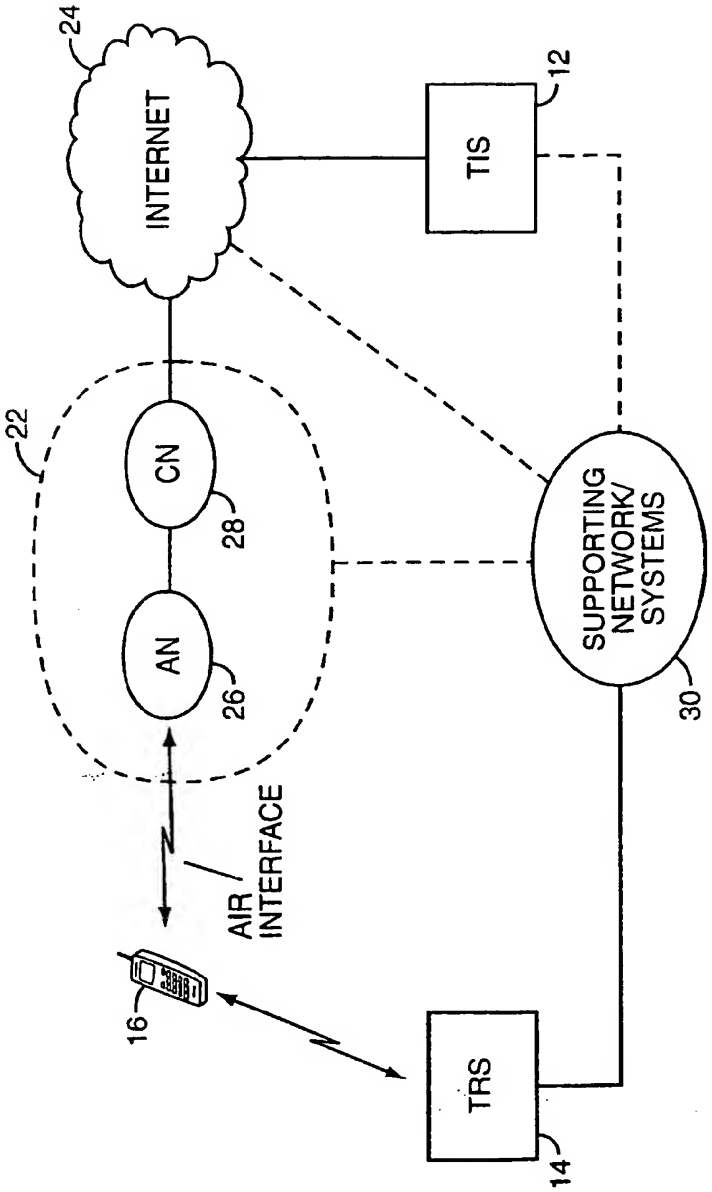
24
INTERNET
12
TIS
22
CN
28
AN
26
SUPPORTING NETWORK/ SYSTEMS
30
AIR INTERFACE
16
TRS
14

FIG. 2

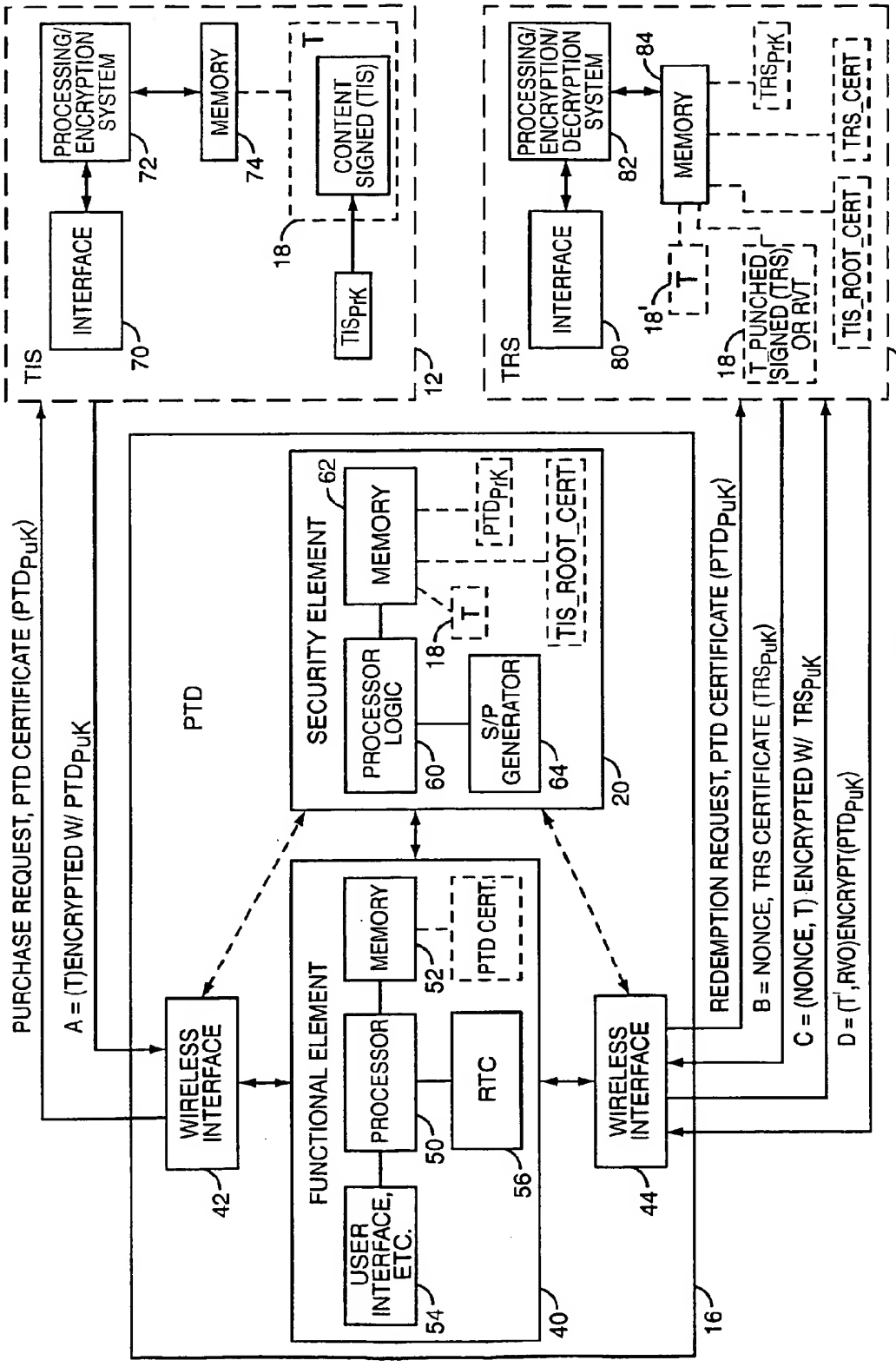
TIS
PROCESSING/ ENCRYPTION SYSTEM
72
MEMORY
74
T
CONTENT SIGNED (TIS)
INTERFACE
70
18
TIS$_{PrK}$
12
TRS
PROCESSING/ ENCRYPTION/ DECRYPTION SYSTEM
82
84
MEMORY
TRS$_{PrK}$
INTERFACE
80
18'
T
T_PUNCHED SIGNED (TRS) OR RVT
18
TIS_ROOT_CERT
TRS_CERT
14
PURCHASE REQUEST, PTD CERTIFICATE (PTD$_{PuK}$)
A = (T)ENCRYPTED W/ PTD$_{PuK}$
PTD
SECURITY ELEMENT
62
MEMORY
PTD$_{PrK}$
PROCESSOR LOGIC
18
T
TIS_ROOT_CERT
S/P GENERATOR
60
64
20
WIRELESS INTERFACE
42
FUNCTIONAL ELEMENT
MEMORY
52
PTD CERT.
PROCESSOR
50
RTC
56
USER INTERFACE, ETC.
54
40
16
WIRELESS INTERFACE
44
REDEMPTION REQUEST, PTD CERTIFICATE (PTD$_{PuK}$)
B = NONCE, TRS CERTIFICATE (TRS$_{PuK}$)
C = (NONCE, T) ENCRYPTED W/ TRS$_{PuK}$
D = (T', RVO)ENCRYPT(PTD$_{PuK}$)

FIG. 3

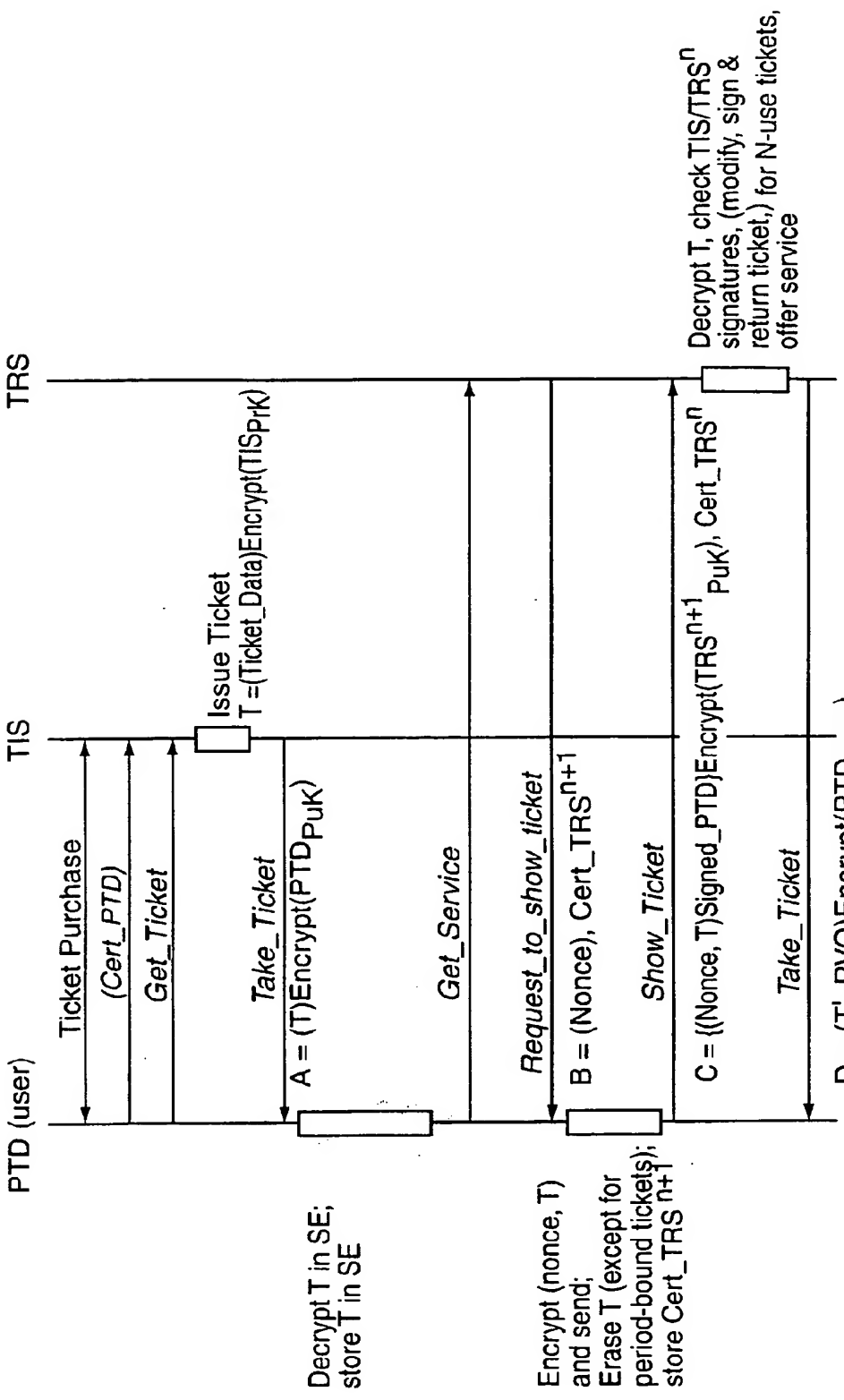
PTD (user)
TIS
TRS
Ticket Purchase
(Cert_PTD)
Get_Ticket
Issue Ticket
T =(Ticket_Data)Encrypt(TIS$_{PrK}$)
Take_Ticket
A = (T)Encrypt(PTD$_{PuK}$)
Get_Service
Request_to_show_ticket
B = (Nonce), Cert_TRS^{n+1}
Show_Ticket
C = {(Nonce, T)Signed_PTD}Encrypt(TRS^{n+1} $_{PuK}$), Cert_TRS^{n}
Take_Ticket
D = (T', RVO)Encrypt(PTD$_{PuK}$)
Decrypt T, check TIS/TRS^{n} signatures, (modify, sign & return ticket,) for N-use tickets, offer service
Decrypt T in SE; store T in SE
Encrypt (nonce, T) and send; Erase T (except for period-bound tickets); store Cert_TRS $^{n+1}$

FIG. 4

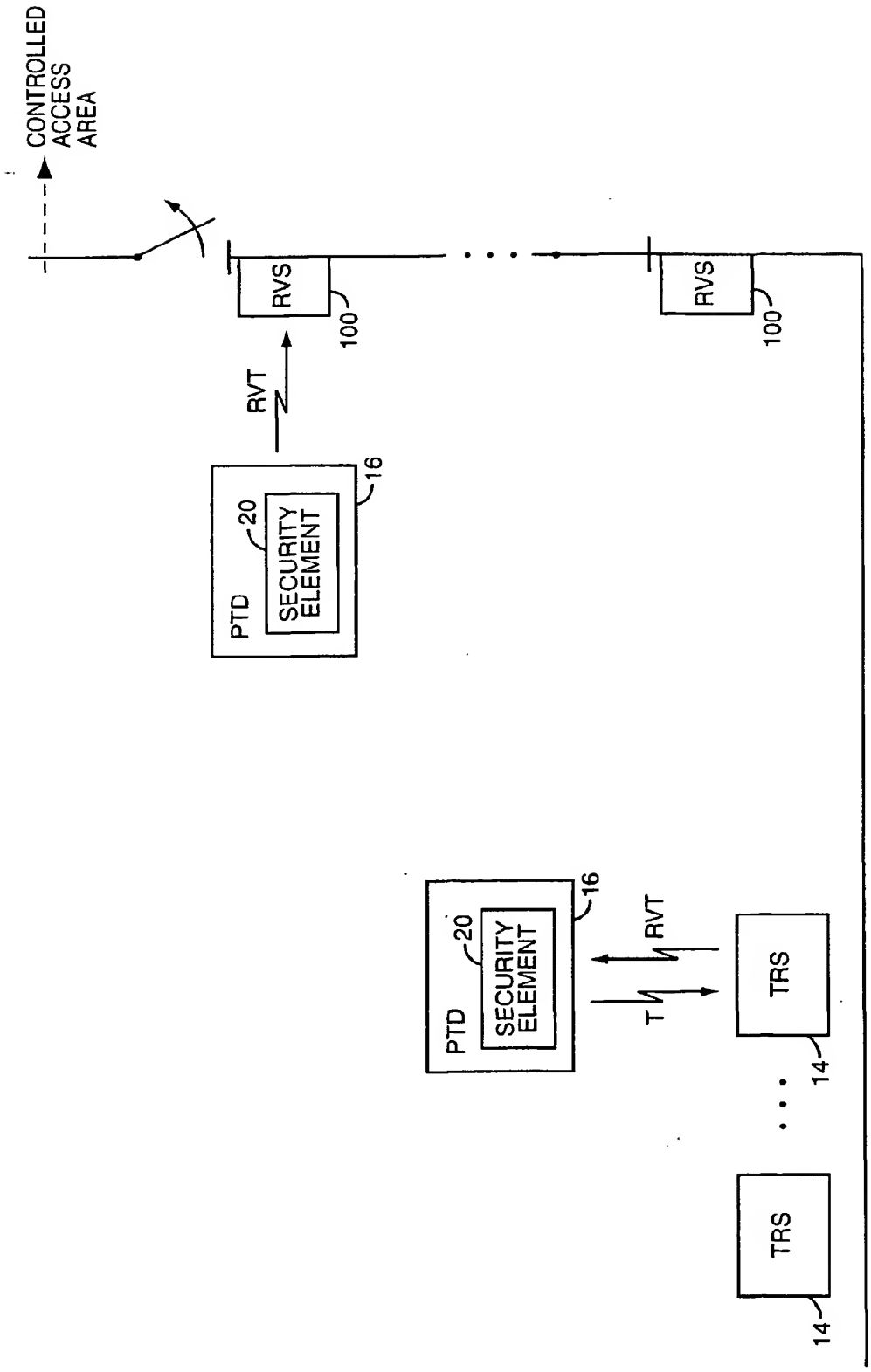
CONTROLLED ACCESS AREA
RVS
100
RVS
100
RVT
PTD
20
SECURITY ELEMENT
16
PTD
20
SECURITY ELEMENT
16
RVT
T
TRS
14
TRS
14

FIG. 5

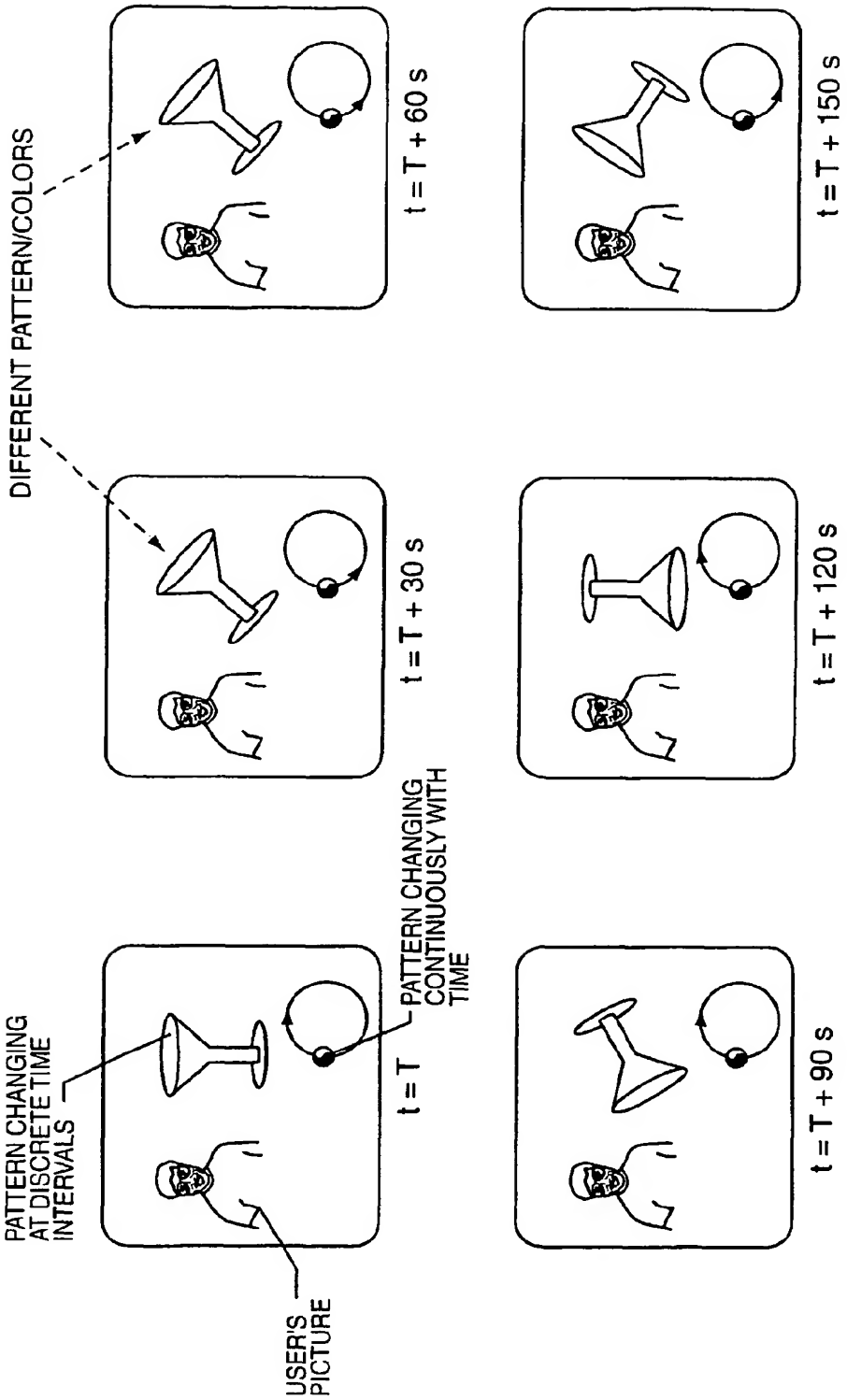
DIFFERENT PATTERN/COLORS
PATTERN CHANGING AT DISCRETE TIME INTERVALS
USER'S PICTURE
PATTERN CHANGING CONTINUOUSLY WITH TIME
t = T
t = T + 30 s
t = T + 60 s
t = T + 90 s
t = T + 120 s
t = T + 150 s

FIG. 6